

A Finite Presentation of CNOT-dihedral Operators

Matthew Amy, Jianxin Chen, Neil J. Ross

Outline

Quantum circuits

Clifford+T and universal gate sets

CNOT-dihedral gates

Rules for CNOT-dihedral gates

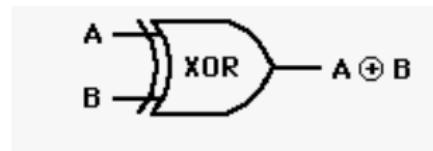
Normal forms

Phase polynomials and uniqueness

Open questions

Classical circuits

- ▶ Logical gates (boolean functions $\mathbb{B}^n \rightarrow \mathbb{B}^m$):

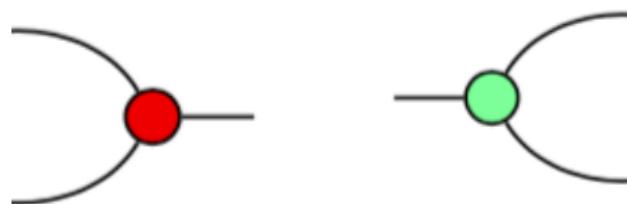


- ▶ Reversible gates (information is physical):

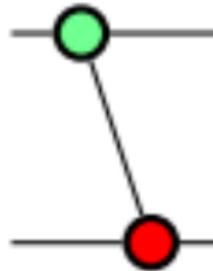


Quantum circuits

- ▶ Logical gates (linear maps $(\mathbb{C}\mathbb{B})^n \rightarrow (\mathbb{C}\mathbb{B})^m$):



- ▶ Reversible gates (unitaries):



Towards an algebraic theory of quantum circuits

Axiomatisations of logical gates (linear maps): ZX, ZW.

Clifford+T is a universal set of (unitary) gates for quantum computing, generated by $\{CNOT, X, H, T\}$.

Want an algebraic theory of reversible (unitary) quantum circuits.

- ▶ Lafont (2003): classical case + affine quantum circuits $\{CNOT, X\}$,
- ▶ Selinger (2015): generators and relations for the Clifford groupoid $\{CNOT, X, H, T^2\}$,
- ▶ Amy et al. (2016): phase polynomials, T-count optimization $\{CNOT, T\}$,
- ▶ The present paper gives generators and relations for CNOT-dihedral groupoid $\{CNOT, X, T\}$.

CNOT-dihedral gates

In the paper, the CNOT-dihedral operators are defined as follows.

Definition 3.1. The *generators* are the scalar $\omega = e^{i\pi/4}$ and the gates X , T , and CNOT defined below.

$$\begin{array}{c} \text{---} \\ \boxed{X} \\ \text{---} \end{array} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{array}{c} \text{---} \\ \boxed{T} \\ \text{---} \end{array} = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix} \quad \begin{array}{c} \text{---} \\ \boxed{X} \\ \text{---} \end{array} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Definition 3.2. The *derived generators* are the gates U and V defined below.

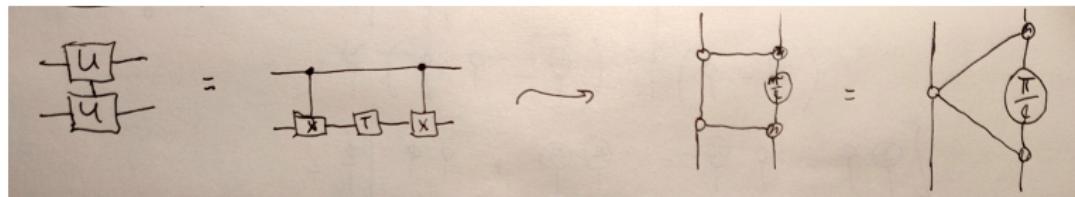
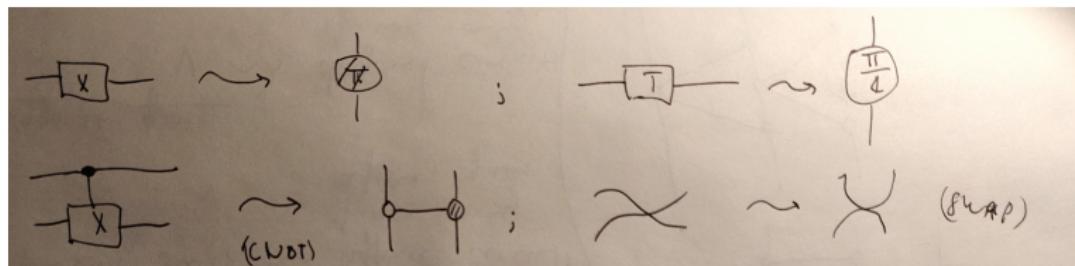
$$\begin{array}{c} \text{---} \\ \boxed{U} \\ \text{---} \\ \boxed{U} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ \boxed{V} \\ \text{---} \\ \boxed{V} \\ \text{---} \\ \boxed{V} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

Figure: Amy, Chen and Ross, p. 86.

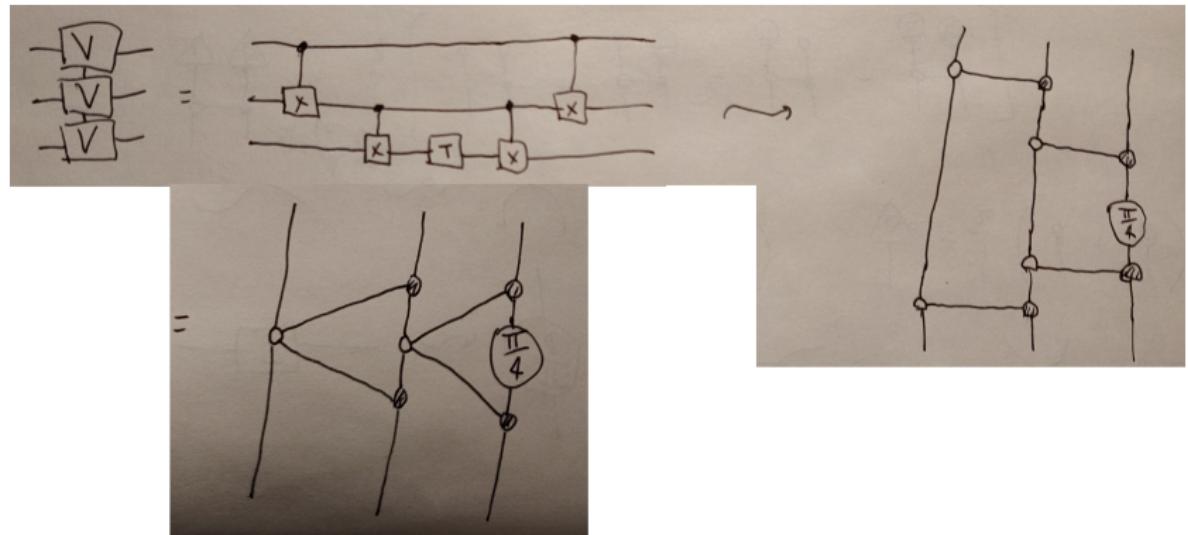
- ▶ The gates X , $CNOT$ and $SWAP$ are called *affine*.
- ▶ The gates ω , T , U and V are called *diagonal*.

CNOT-dihedral gates in ZX

The gates can be expressed in the ZX-calculus.



CNOT-dihedral gates in ZX



Rules for CNOT-dihedral gates

$$R_1 : \boxed{X^2} = \underline{\hspace{1cm}}$$

$$R_2 : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \quad \boxed{X} \quad \boxed{X} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array}$$

$$R_3 : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array}$$

$$R_4 : \begin{array}{c} \text{---} \\ | \\ \boxed{X^2} \\ | \\ \text{---} \end{array} = \underline{\hspace{1cm}}$$

$$R_5 : \begin{array}{c} \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \boxed{X} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array}$$

$$R_6 : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \\ | \\ \text{---} \\ | \\ \boxed{X} \\ | \\ \text{---} \\ | \\ \boxed{X} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

$$R_7 : \boxed{T^8} = \underline{\hspace{1cm}}$$

$$R_8 : \begin{array}{c} \boxed{U^4} \\ | \\ \boxed{U^4} \end{array} = \begin{array}{c} \boxed{T^4} \\ | \\ \boxed{T^4} \end{array}$$

$$R_9 : \begin{array}{c} \boxed{V^2} \\ | \\ \boxed{V^2} \\ | \\ \boxed{V^2} \end{array} = \begin{array}{c} \boxed{T^6} \quad \boxed{U^2} \quad \boxed{U^2} \\ | \\ \boxed{T^6} \quad \boxed{U^2} \quad \boxed{U^2} \\ | \\ \boxed{T^6} \quad \boxed{U^2} \quad \boxed{U^2} \end{array}$$

$$R_{10} : \omega^8 =$$

$$R_{11} : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \quad \boxed{T} \quad \boxed{X} \\ | \\ \text{---} \end{array} = \omega \begin{array}{c} \text{---} \\ | \\ \boxed{T^7} \\ | \\ \text{---} \end{array}$$

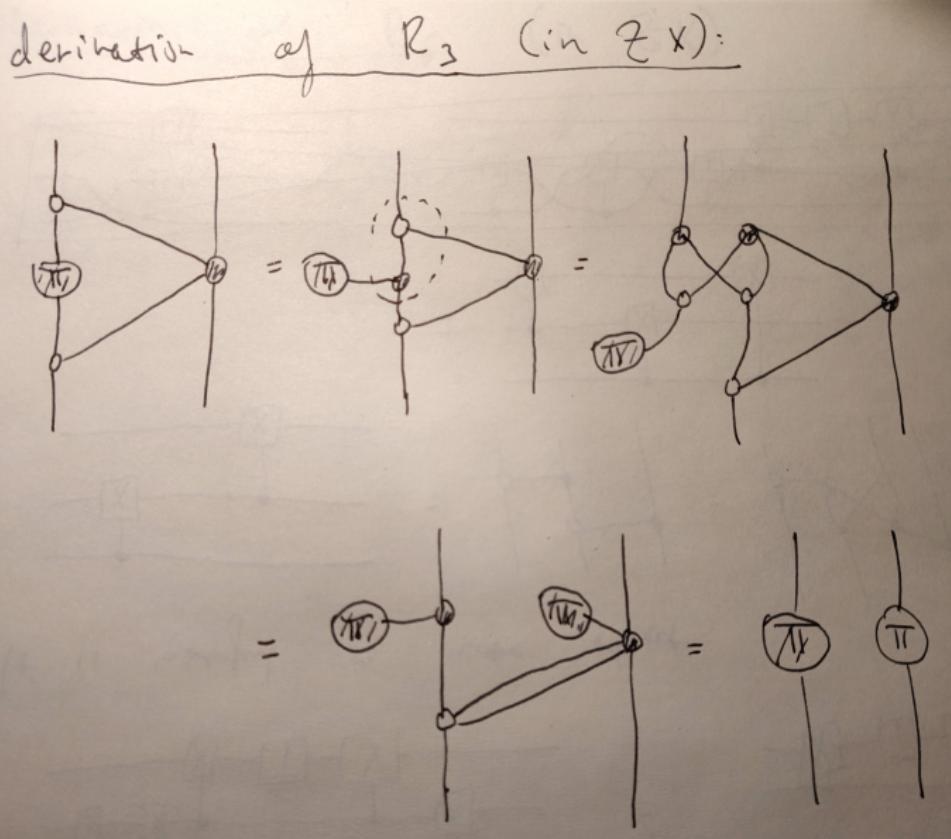
$$R_{12} : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \quad \boxed{T} \quad \boxed{X} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{T} \\ | \\ \text{---} \end{array}$$

$$R_{13} : \begin{array}{c} \text{---} \\ | \\ \boxed{X} \quad \boxed{V} \quad \boxed{X} \\ | \\ \boxed{V} \\ | \\ \boxed{V} \end{array} = \begin{array}{c} \text{---} \\ | \\ \boxed{T^5} \quad \boxed{U^3} \quad \boxed{U^3} \quad \boxed{U^3} \\ | \\ \boxed{T^5} \quad \boxed{U^3} \\ | \\ \boxed{T^5} \quad \boxed{U^3} \quad \boxed{U^3} \quad \boxed{U^3} \\ | \\ \boxed{T^5} \quad \boxed{U^3} \quad \boxed{U^3} \quad \boxed{U^3} \\ | \\ \boxed{V} \quad \boxed{V} \quad \boxed{V} \\ | \\ \boxed{V} \quad \boxed{V} \quad \boxed{V} \\ | \\ \boxed{V} \quad \boxed{V} \quad \boxed{V} \end{array}$$

Figure 1: The relations. R_1 through R_6 are affine relations. R_7 through R_{10} are diagonal relations. R_{11} through R_{12} are commutation relations.

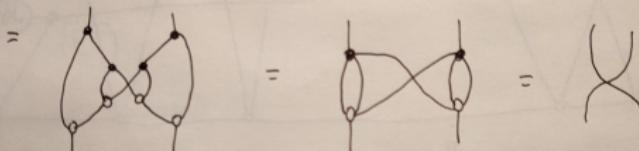
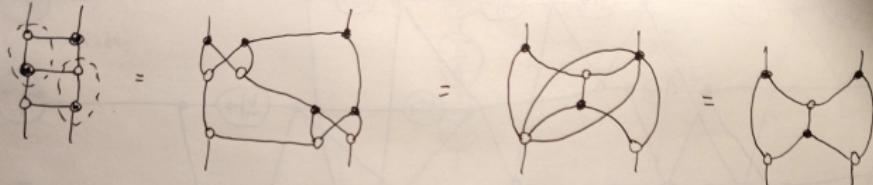
Figure: Amy, Chen and Ross, p. 87.

Derivation of R3 ZX

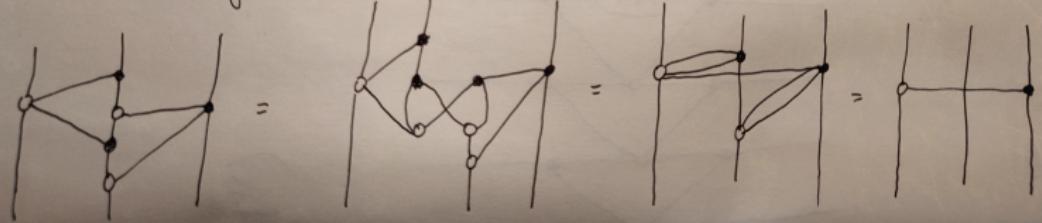


Derivation of R5 and R6 in ZX

derivation of R₅ (in ZX)



derivation of R₆

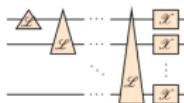


Commutation rules

$$\begin{array}{c} \text{Top row: } \\ \begin{array}{ccc} \text{Diagram: } X \text{ (orange)} \otimes T \text{ (pink)} & = \omega \cdot & \text{Diagram: } T^* \text{ (pink)} \otimes X \text{ (orange)} \\ \text{Diagram: } X \text{ (orange)} \otimes U \text{ (purple)} & = \omega \cdot & \text{Diagram: } U^* \text{ (purple)} \otimes X \text{ (orange)} \\ \text{Diagram: } X \text{ (orange)} \otimes V \text{ (green)} & = \omega \cdot & \text{Diagram: } V^* \text{ (green)} \otimes X \text{ (orange)} \end{array} \\ \begin{array}{ccc} \text{Diagram: } X \text{ (orange)} \otimes U^* \text{ (purple)} & = \omega \cdot & \text{Diagram: } U \text{ (purple)} \otimes U^* \text{ (purple)} \\ \text{Diagram: } X \text{ (orange)} \otimes V^* \text{ (green)} & = \omega \cdot & \text{Diagram: } V \text{ (green)} \otimes V^* \text{ (green)} \\ \text{Diagram: } X \text{ (orange)} \otimes V \text{ (green)} & = \omega \cdot & \text{Diagram: } V^* \text{ (green)} \otimes X \text{ (orange)} \end{array} \end{array}$$
$$\begin{array}{c} \text{Second row: } \\ \begin{array}{ccc} \text{Diagram: } X \text{ (orange)} \otimes T \text{ (pink)} & = & \text{Diagram: } T \text{ (pink)} \otimes X \text{ (orange)} \\ \text{Diagram: } X \text{ (orange)} \otimes U \text{ (purple)} & = & \text{Diagram: } U \text{ (purple)} \otimes X \text{ (orange)} \\ \text{Diagram: } X \text{ (orange)} \otimes U^* \text{ (purple)} & = & \text{Diagram: } U^* \text{ (purple)} \otimes X \text{ (orange)} \end{array} \\ \begin{array}{ccc} \text{Diagram: } X \text{ (orange)} \otimes V \text{ (green)} & = & \text{Diagram: } V \text{ (green)} \otimes X \text{ (orange)} \\ \text{Diagram: } X \text{ (orange)} \otimes V^* \text{ (green)} & = & \text{Diagram: } V^* \text{ (green)} \otimes X \text{ (orange)} \\ \text{Diagram: } X \text{ (orange)} \otimes V \text{ (green)} & = & \text{Diagram: } V \text{ (green)} \otimes X \text{ (orange)} \end{array} \end{array}$$
$$\begin{array}{c} \text{Third row: } \\ \begin{array}{ccc} \text{Diagram: } X \text{ (orange)} \otimes V \text{ (green)} & = & \text{Diagram: } U \text{ (purple)} \otimes X \text{ (orange)} \\ \text{Diagram: } X \text{ (orange)} \otimes V^* \text{ (green)} & = & \text{Diagram: } U^* \text{ (purple)} \otimes X \text{ (orange)} \\ \text{Diagram: } X \text{ (orange)} \otimes V \text{ (green)} & = & \text{Diagram: } V \text{ (green)} \otimes X \text{ (orange)} \end{array} \\ \begin{array}{c} \text{Fourth row: } \\ \begin{array}{c} \text{Diagram: } X \text{ (orange)} \otimes V \text{ (green)} = T^* \otimes U \otimes U^* \otimes U^* \otimes V \otimes V \otimes V \otimes X \\ \text{Diagram: } X \text{ (orange)} \otimes V \text{ (green)} = T^* \otimes U^3 \otimes U^3 \otimes U^3 \otimes U^3 \otimes V \otimes V \otimes V \otimes X \end{array} \end{array} \end{array}$$
$$\begin{array}{c} \text{Bottom row: } \\ \begin{array}{ccc} \text{Diagram: } T \text{ (pink)} \otimes X & = & \text{Diagram: } T \text{ (pink)} \otimes X \\ \text{Diagram: } U \text{ (purple)} \otimes X & = & \text{Diagram: } U \text{ (purple)} \otimes X \\ \text{Diagram: } V \text{ (green)} \otimes X & = & \text{Diagram: } V \text{ (green)} \otimes X \end{array} \\ \begin{array}{ccc} \text{Diagram: } T \text{ (pink)} \otimes X & = & \text{Diagram: } T \text{ (pink)} \otimes X \\ \text{Diagram: } U \text{ (purple)} \otimes X & = & \text{Diagram: } U \text{ (purple)} \otimes X \\ \text{Diagram: } V \text{ (green)} \otimes X & = & \text{Diagram: } V \text{ (green)} \otimes X \end{array} \\ \begin{array}{ccc} \text{Diagram: } T \text{ (pink)} \otimes X & = & \text{Diagram: } T \text{ (pink)} \otimes X \\ \text{Diagram: } U \text{ (purple)} \otimes X & = & \text{Diagram: } U \text{ (purple)} \otimes X \\ \text{Diagram: } V \text{ (green)} \otimes X & = & \text{Diagram: } V \text{ (green)} \otimes X \end{array} \end{array}$$

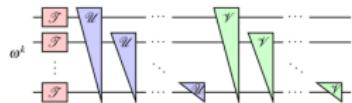
Normal forms

Definition 4.3. An *affine normal form* is a circuit A of the form



such that $\deg_X(A) \in \mathbb{Z}_2$ and $\deg_{\text{CNOT}}(A) \in \mathbb{Z}_2$.

Definition 4.8. A *diagonal normal form* is a circuit D of the form



such that $k \in \mathbb{Z}_8$, $\deg_T(D) \in \mathbb{Z}_8$, $\deg_U(D) \in \mathbb{Z}_4$, and $\deg_V(D) \in \mathbb{Z}_2$.

- ▶ Degrees in the normal forms reflect the degree reduction rules.
- ▶ Every affine circuit admits a unique normal form (Lafont, 2003).
- ▶ Every diagonal circuit admits a normal form (Lemma 5.3.)
- ▶ Every CNOT-dihedral circuit C admits a normal form $C = DA$, where D is a diagonal circuit in normal form and A is an affine circuit in normal form.

Phase polynomials

Action of a diagonal gate:

$$D |x\rangle = \omega^{p_D(x)} |x\rangle, \quad p_D : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_8,$$

$$\omega^k |x\rangle = \omega^k |x\rangle$$

$$T^k |x_1\rangle = \omega^{kx_1} |x_1\rangle$$

$$U^k |x_1 x_2\rangle = \omega^{k(x_1 \oplus x_2)} |x_1 x_2\rangle$$

$$V^k |x_1 x_2 x_3\rangle = \omega^{k(x_1 \oplus x_2 \oplus x_3)} |x_1 x_2 x_3\rangle$$

Therefore for D in normal form we have

$$p_D(x) = a_0 + \sum_i a_i x_i + \sum_{i < j} b_{ij}(x_i \oplus x_j) + \sum_{i < j < k} c_{ijk}(x_i \oplus x_j \oplus x_k)$$

Where $a_i \in \mathbb{Z}_8$, $b_{ij} \in \mathbb{Z}_4$, $c_{ijk} \in \mathbb{Z}_2$ (from the bounds on $\deg_X(D)$ for $X = T, U, V$ obtained in normal form).

Uniqueness

Suppose D and D' are distinct diagonal normal forms, we want to show that $\exists y \in \mathbb{Z}^2$ such that $D|y\rangle \neq D'|y\rangle$.

By construction $p_D(x) \neq p_{D'}(x)$ as polynomials. However this does not mean that $\exists y \in \mathbb{Z}_2^n$ s.t. $p_D(y) \neq p_{D'}(y)$.

Counterexample: $4x_1 + 4x_2 + 4(x_1 \oplus x_2) = 0 \bmod 8$ for any $x_1, x_2 \in \mathbb{Z}_2$

The existence of such a y comes from the bounds on the coefficients a_i , b_{ij} and c_{ijk} .

Construct a multilinear polynomial $q : \mathbb{Z}_8^n \rightarrow \mathbb{Z}_8$ such that $p_D(y) - p_{D'}(y) = q(y) \forall y \in \mathbb{Z}_2^n$.

Do this by translating from mod 2 to mod 8:

$$x_i \oplus x_j = x_i + x_j - 2x_i x_j$$

$$x_i \oplus x_j \oplus x_k = x_i + x_j + x_k - 2x_i x_j - 2x_i x_k - 2x_j x_k + 4x_i x_j x_k$$

Then $p_D(x) - p_{D'}(x) \neq 0 \implies q(x) \neq 0$, because of the bounds on a_i , b_{ij} and c_{ijk} . Pick a non-zero term $d x_{i_1} \dots x_{i_k}$ in $q(x)$ and let y have 1's in i_j th positions and zero everywhere else. Then $q(y) = d \neq 0$ and so $D|y\rangle \neq D'|y\rangle$.

Open questions

- ▶ Interaction between ZX and CNOT-dihedral rules (rule 13?).
- ▶ Phase polynomials representations for graph rewriting.
- ▶ Algebraic vs combinatorial description: the paper doesn't contain an algorithm for normalizing CNOT-dihedral circuits, it uses the properties of the ambient symmetric monoidal structure non-constructively. What would be a rewrite system?
- ▶ Complexity of CNOT-dihedral circuits: word problem for CNOT-dihedral circuits? Classical simulation of the normal form?